

AN IMMUNE SYSTEM FOR COMPUTERS

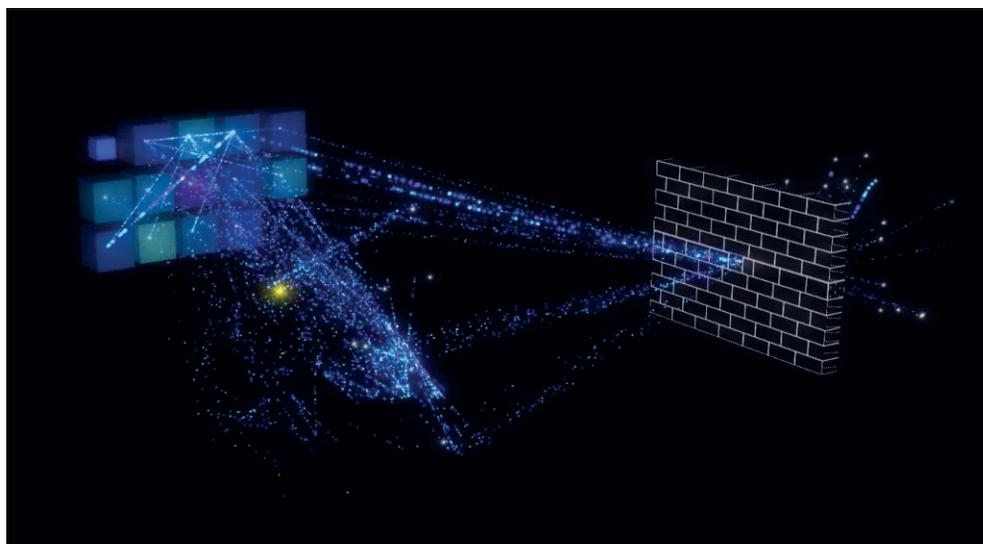
Darktrace has developed AI software designed to detect and defend against cyber threats from within computer networks – an immune system for computers.

Darktrace was established by Poppy Gustafsson and Jack Stockdale in 2013 when cyber intelligence experts from the US and the UK teamed up with mathematicians from the University of Cambridge. The resulting company was established to find new ways of protecting computer systems from malicious attacks. Its technology has gone on to be used by over 3,000 organisations of all sizes and scale, including Prudential, Suzuki and the US Department of Homeland Security.

Traditionally, cybersecurity relied on historical data of detectable signatures and rules, to spot and block threats. However, novel malware would not have a track record and could enter computer systems undetected. Darktrace counters this legacy approach by using artificial intelligence to create a self-learning cyber immune system. This defends all types of networks, including physical, cloud and virtual environments, the Internet of Things and industrial control systems.

Darktrace can be deployed on a company's network within minutes and uses Bayesian algorithms to apply probabilistic statistical reasoning to cybersecurity. The technology learns the normal 'pattern of life' of every user and device on a network, flagging suspicious activity with a percentage score of how likely it is to be a genuine threat. It provides an evolving cyber immune system that knows the usual activities of the organisation it sits within, meaning it can detect and, where necessary, contain the threat while enabling the system to continue running.

Darktrace's Cyber AI platform is powered by unsupervised machine learning, and was the first software of its type. The engineering



Threat visualiser subnet view. One of the strengths of Darktrace is to present a simple interface that can then be drilled down upon so that the users know when to take action © Darktrace

challenge faced was in both speed and scale of analysis. Up to 100 million packets per second (a measure of throughput for network devices including bridges, routers and switches) needed to be analysed in real time to be effective.

Darktrace's Autonomous Response Antigena technology launched in 2016, providing – for the first time in the industry – the possibility of a 'self-healing' network. The technology works by harnessing the power and precision of Darktrace's threat detection, to calculate an effective but proportionate response to an in-progress attack. Once the AI has identified threatening activity that reaches a certain threshold of severity, its algorithms generate a real-time action that enforces the 'pattern of life' of the device or user affected, protecting the system from an emerging threat. This might involve interrupting specific, suspicious connections, automatically reconfiguring a part of the

network or temporarily freezing certain user privileges. These reactions only target the threatening behaviour, so business elsewhere on the system can continue as usual.

Antigena was a MacRobert Award finalist in 2019, following the Enterprise Immune System's success in reaching the last three contenders in 2017. The company has seen huge take-up since it acquired its first client Drax, the electrical power generation company. Darktrace's technology is now being used by over 3,000 organisations across 110 countries, including the digital estates of government agencies, international banks, healthcare providers and telecoms operators.

Darktrace's rapid growth over six years has seen its valuation rise to over \$1.65 billion, with offices in 44 countries employing over one thousand people.

For more information see: www.darktrace.com